Raspodijeljene glavne knjige i kriptovalute

Pametni ugovori na Ethereum platformi, jezik Solidity

Ante Đerek, Zvonko Konstanjčar

10. prosinca 2021.

Druga vježba: Pametni ugovori u jeziku Solidity

- Ako radite u paru, prijava do 15.12.2021. u 23:59h.
- Rok za predaju putem MS Teams-a: 19.12.2021. u 23:59h.
- Konzultacije: putem MS Team-a po dogovoru – `rgkk@fer.hr`
- Ocjenjivanje: izvorni kod, obrana uživo

Naučite Solidity!

Završni ispit pretpostavlja znanje Solidity-ja potrebno za izradu vježbe.

Literatura

- Mastering Ethereum, Andreas M. Antonopoulos, Gavin Wood, dostupna na `https://github.com/ethereumbook/ethereumbook/`
- Solidity documentation, dostupna na `https://solidity.readthedocs.io/en/latest/`

Također zanimljivo:

- Ethereum whitepaper, Vitalik Buterin, dostupan na `https://ethereum.org/en/whitepaper/`
- Ethereum yellowpaper, Gawin Wood, dostupan na `https://ethereum.github.io/yellowpaper/paper.pdf`

Nick Szabo (1996)

A set of promises, specified in digital form, including protocols within which the parties perform on other promises.

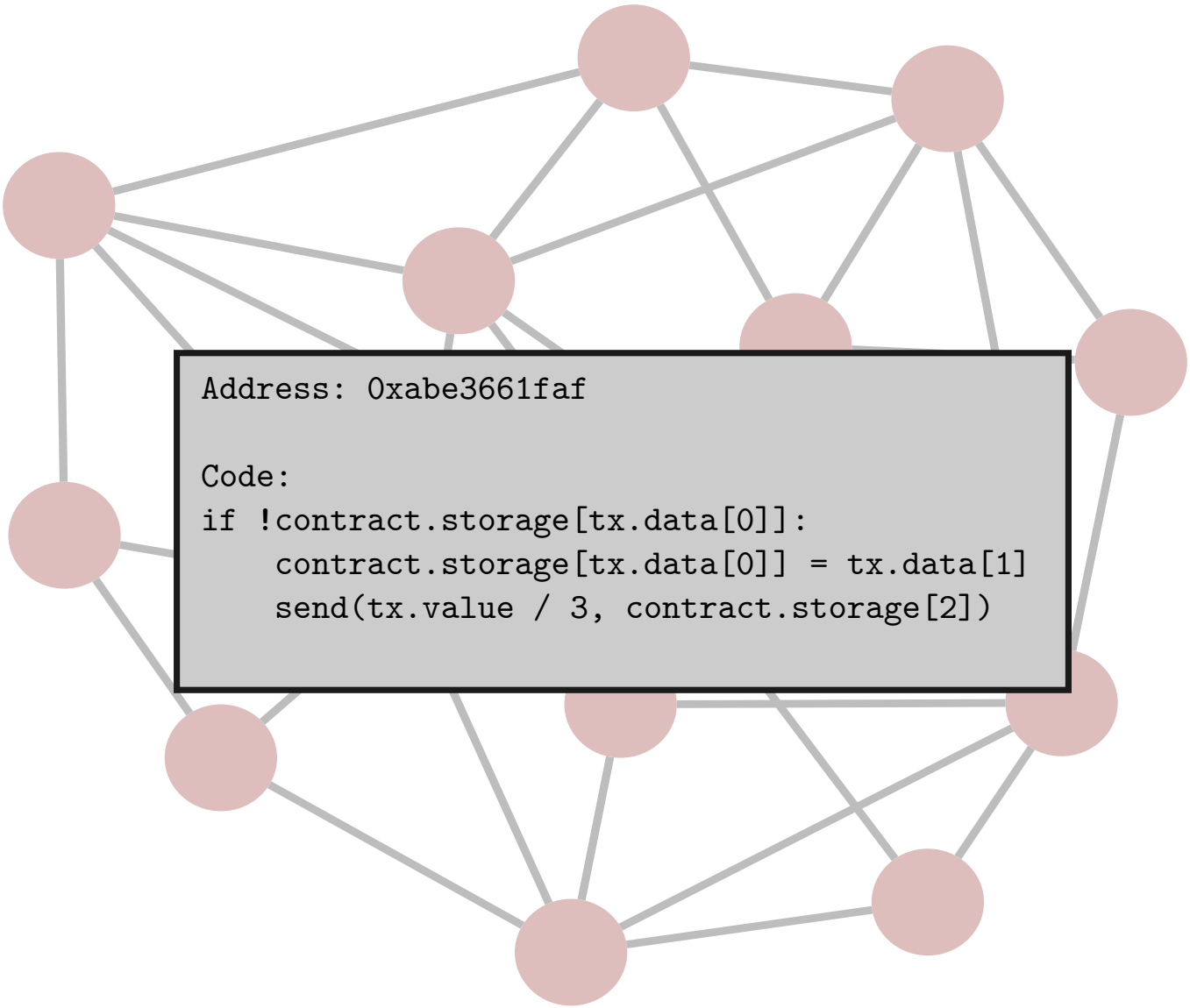
ethereum.org (2018)

Applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

Definicija

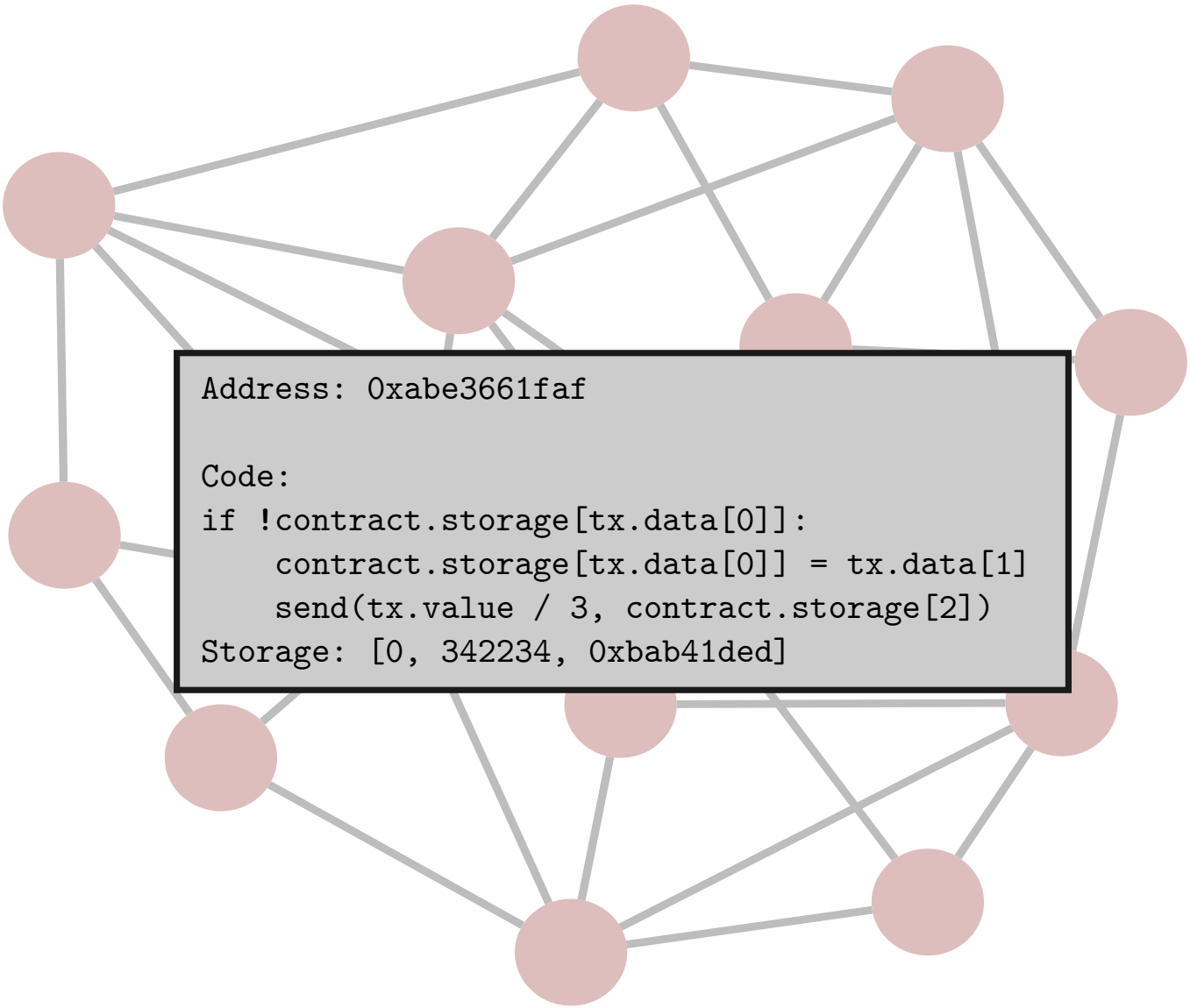
Pametni ugovor je javni i nepromjenjivi računalni program koji je pohranjen na kriptografskom lancu blokova i koji se može javno i pouzdano izvršavati koristeći kriptografski lanac blokova i distribuirani konsenzus.

Pametni ugovori – javni i nepromijenjivi



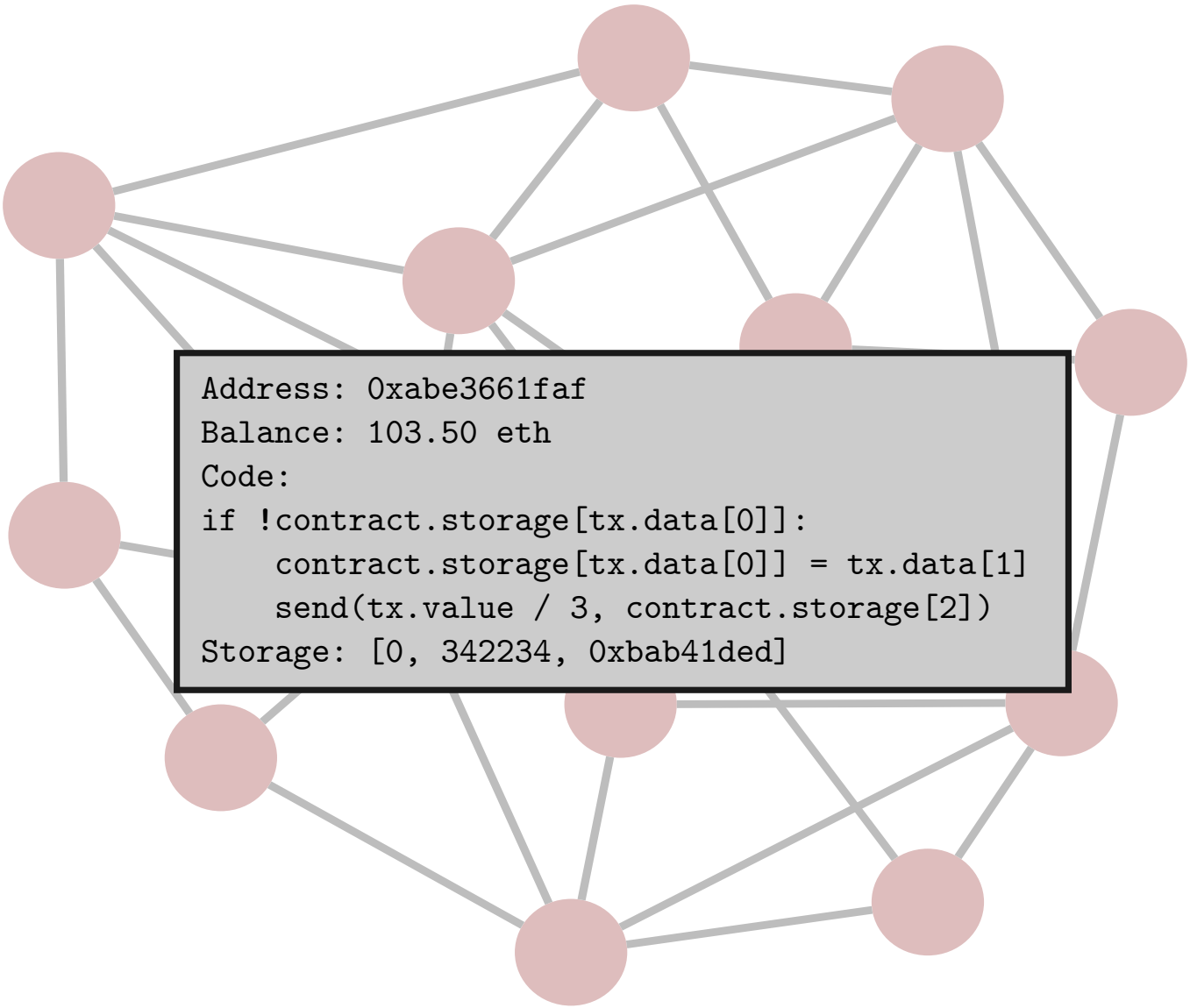
```
Address: 0xabe3661faf

Code:
if !contract.storage[tx.data[0]]:
    contract.storage[tx.data[0]] = tx.data[1]
    send(tx.value / 3, contract.storage[2])
```

Pametni ugovori – mogu pohraniti informacije



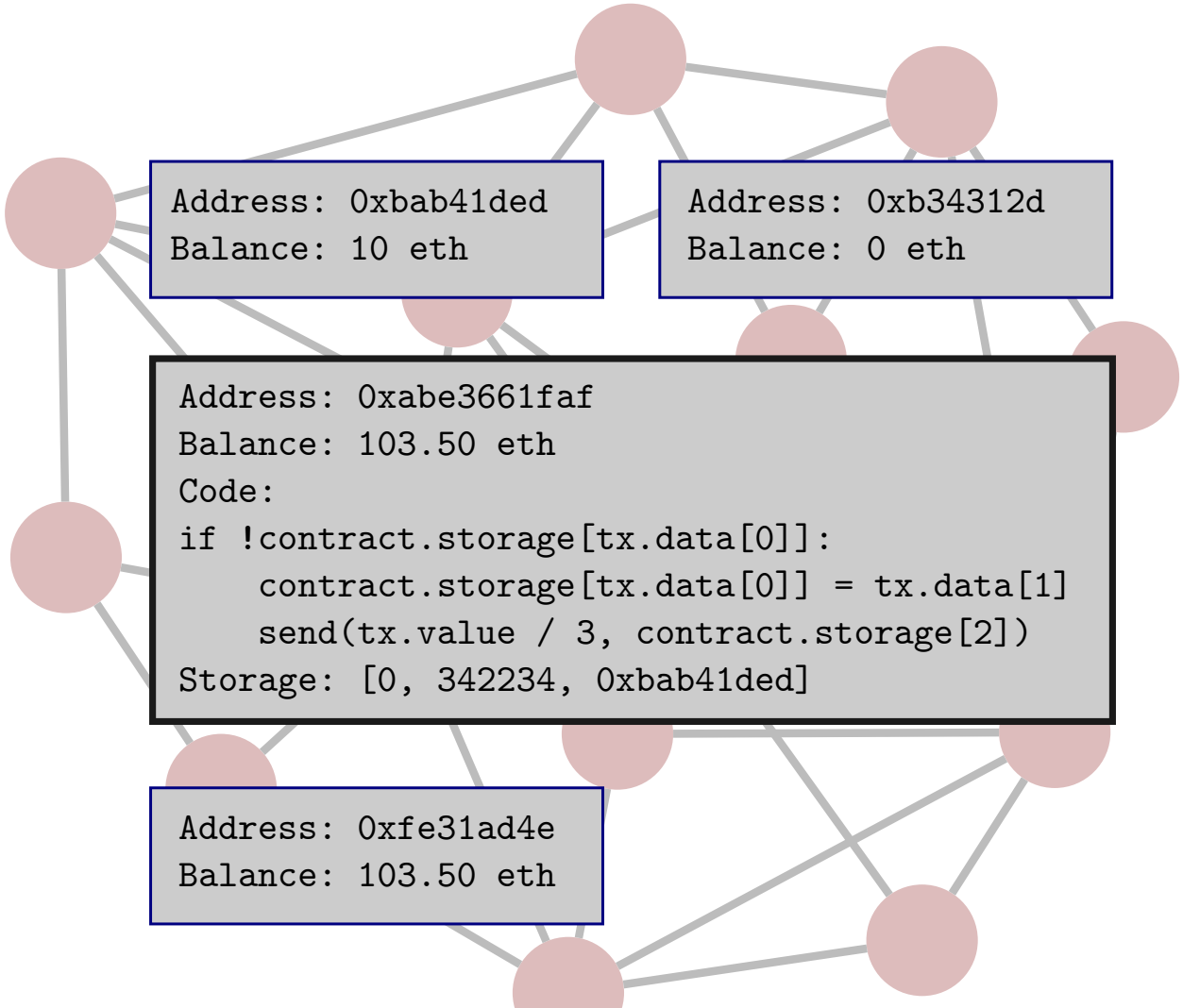
```
Address: 0xabe3661faf

Code:
if !contract.storage[tx.data[0]]:
    contract.storage[tx.data[0]] = tx.data[1]
    send(tx.value / 3, contract.storage[2])
Storage: [0, 342234, 0xbab41ded]
```

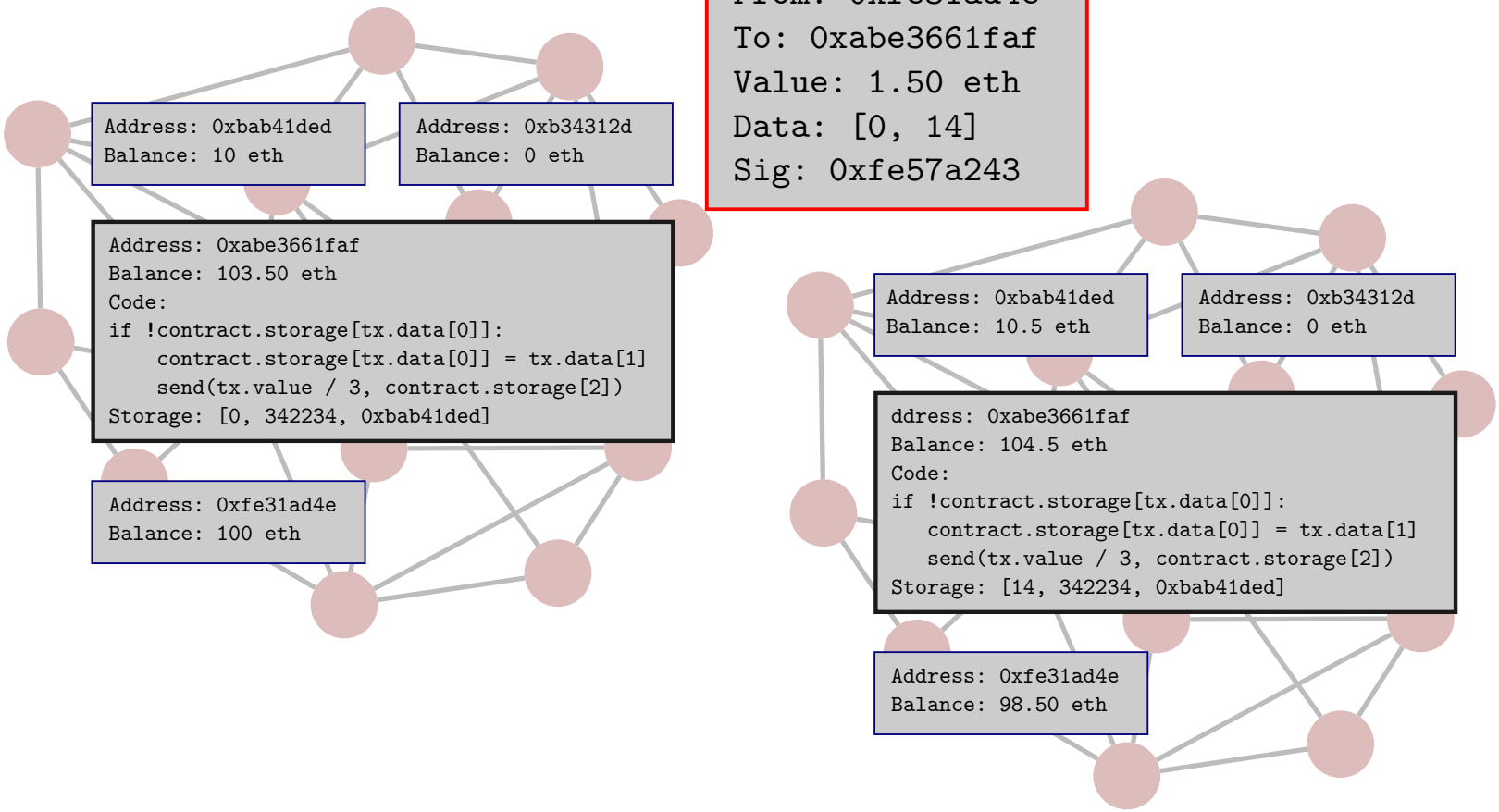
Pametni ugovori – vlasnici kriptovalute



```
Address: 0xabe3661faf
Balance: 103.50 eth
Code:
if !contract.storage[tx.data[0]]:
    contract.storage[tx.data[0]] = tx.data[1]
    send(tx.value / 3, contract.storage[2])
Storage: [0, 342234, 0xbab41ded]
```

- Vanjski račun (*externally owned account*)
- Pametni ugovor (*contract*)




Address: 0xbab41ded
Balance: 10 eth
Address: 0xb34312d
Balance: 0 eth
Address: 0xabe3661faf
Balance: 103.50 eth
Code:
if !contract.storage[tx.data[0]]:
contract.storage[tx.data[0]] = tx.data[1]
send(tx.value / 3, contract.storage[2])
Storage: [0, 342234, 0xbab41ded]
Address: 0xfe31ad4e
Balance: 100 eth
From: 0xfe31ad4e
To: 0xabe3661faf
Value: 1.50 eth
Data: [0, 14]
Sig: 0xfe57a243
Address: 0xbab41ded
Balance: 10.5 eth
Address: 0xb34312d
Balance: 0 eth
ddress: 0xabe3661faf
Balance: 104.5 eth
Code:
if !contract.storage[tx.data[0]]:
contract.storage[tx.data[0]] = tx.data[1]
send(tx.value / 3, contract.storage[2])
Storage: [14, 342234, 0xbab41ded]
Address: 0xfe31ad4e
Balance: 98.50 eth

Globalno stanje kriptografskog lanca blokova

- Za svaki vanjski račun:
  - Iznos kriptovalute.
- Za svaki ugovor:
  - Iznos kriptovalute.
  - Sadržaj memorije.

Transakcija

Transakcija mijenja globalno stanje.

- Obične transakcije: prebacuju kriptovalutu.
- Pozivi ugovora: izvršavaju program ugovora.

Izvor transakcije je uvijek *vanjski* račun!

Zadatak

Osmislite pametni ugovor koji će služiti kao fond za Mirkovo fakultetsko obrazovanje i koji će imati sljedeća svojstva:

- *Svatko može uplatiti novac u fond.*
- *Mirko može podići novac kada navrši 18 godina.*
- *Mirkovi roditelji mogu podići novac bilo kada, ako to oboje zatraže.*

Zadatak

Tko je vlasnik ugovora kojeg ste osmislili i kako možemo implementirati vlasništvo ugovora?

Zadatak

Proširite problem na proizvoljan način i prilagodite dizajn.

Izražajnost ugovora (najčešće) nije ograničena

Prilikom izvršavanja ugovor može:

- računati bilo što (jezik je *Turing potpun*),
- slati kriptovalutu,
- pozivati druge ugovore.

Ugovor se izvršava u *ograničenom* kontekstu

Ako transakcija T poziva ugovor C, ugovoru su dostupni samo:

- trajna memorija ugovora C,
- podaci iz transakcije T,
- izvor transakcije T (autentificiran digitalnim potpisom),
- metapodaci iz trenutnog i nedavnih blokova,
- rezultati eventualnih poziva drugih ugovora od strane C-a.

Želimo konsenzus oko ispravnog izvršavanja!

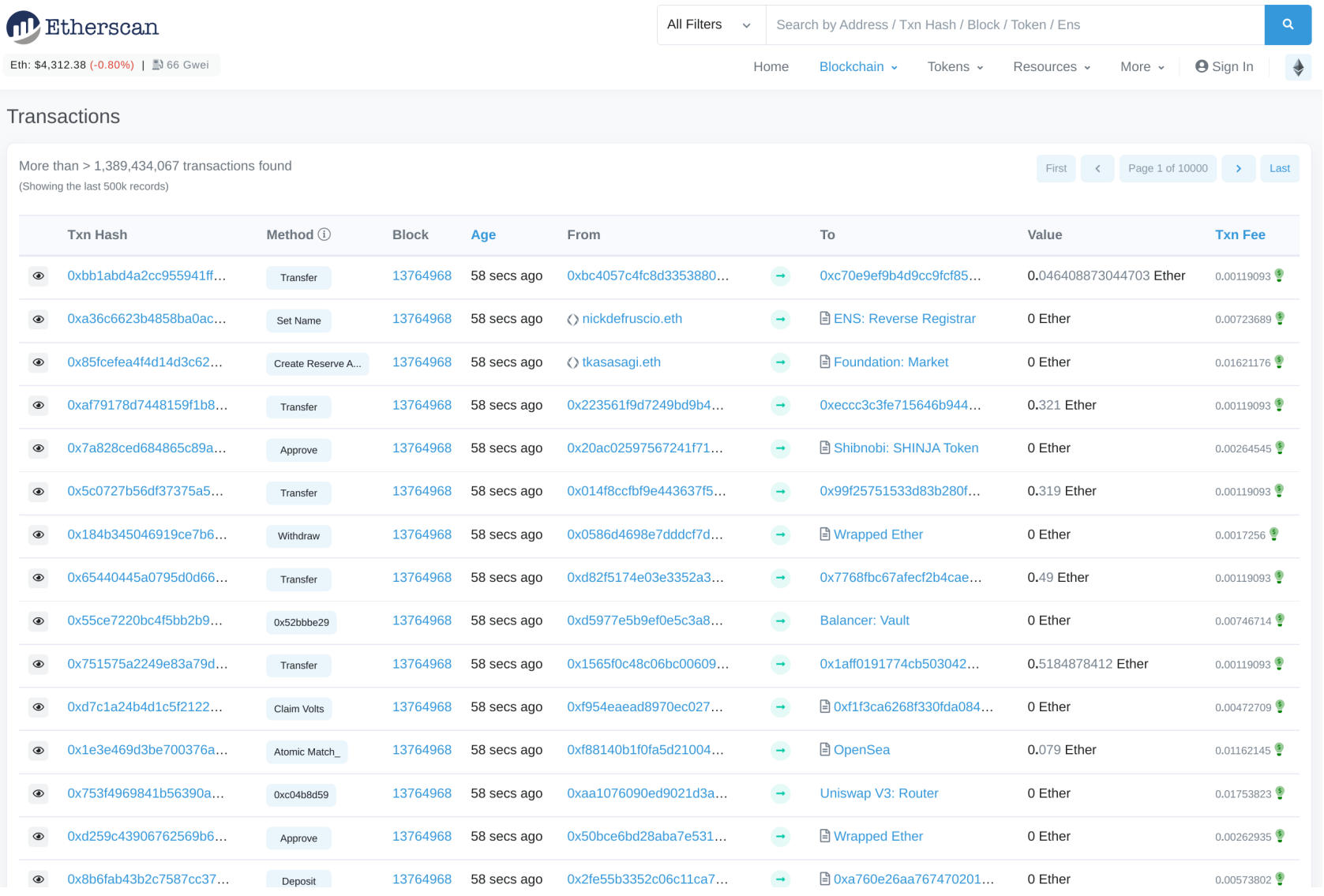
Čvorovi mreže se moraju usaglasiti:

- je li poziv svaki ugovora izvršen ispravno,
- kojim su redoslijedom izvršene transakcije,
- koji je rezultat izvršavanja transakcija odnosno ugovora.

Kako postići raspodijeljeni konsenzus?

- Niz transakcija zajedno s krajnjim globalnim stanjem čini *blok*.
- Rudari izvršavaju pozive ugovora prilikom slaganja bloka.
- Distribuirani konsenzus slično kao kod "običnih" kriptovaluta (*proof-of-work*).

Pametni ugovori – Etherscan



Etherscan

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Eth: $4,312.38 (-0.80%) | 66 Gwei

Home | Blockchain | Tokens | Resources | More | Sign In

Transactions

More than > 1,389,434,067 transactions found

(Showing the last 500k records)

First | Page 1 of 10000 | Last

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0xbb1abd4a2cc955941ff…	Transfer	13764968	58 secs ago	0xbc4057c4fc8d3353880…	0xc70e9ef9b4d9cc9fcf85…	0.046408873044703 Ether	0.00119093
0xa36c6623b4858ba0ac…	Set Name	13764968	58 secs ago	nickdefruscio.eth	ENS: Reverse Registrar	0 Ether	0.00723689
0x85fcefea4f4d14d3c62…	Create Reserve A...	13764968	58 secs ago	tkasasagi.eth	Foundation: Market	0 Ether	0.01621176
0xaf79178d7448159f1b8…	Transfer	13764968	58 secs ago	0x223561f9d7249bd9b4…	0xeccc3c3fe715646b944…	0.321 Ether	0.00119093
0x7a828ced684865c89a…	Approve	13764968	58 secs ago	0x20ac0259756724 1f71…	Shibnobi: SHINJA Token	0 Ether	0.00264545
0x5c0727b56df37375a5…	Transfer	13764968	58 secs ago	0x014f8ccfbf9e443637f5…	0x99f25751533d83b280f…	0.319 Ether	0.00119093
0x184b345046919ce7b6…	Withdraw	13764968	58 secs ago	0x0586d4698e7dddcf7d…	Wrapped Ether	0 Ether	0.0017256
0x65440445a0795d0d66…	Transfer	13764968	58 secs ago	0xd82f5174e03e3352a3…	0x7768fbc67afecf2b4cae…	0.49 Ether	0.00119093
0x55ce7220bc4f5bb2b9…	0x52bbbe29	13764968	58 secs ago	0xd5977e5b9ef0e5c3a8…	Balancer: Vault	0 Ether	0.00746714
0x751575a2249e83a79d…	Transfer	13764968	58 secs ago	0x1565f0c48c06bc00609…	0x1aff0191774cb503042…	0.5184878412 Ether	0.00119093
0xd7c1a24b4d1c5f2122…	Claim Volts	13764968	58 secs ago	0xf954eaead8970ec027…	0xf1f3ca6268f330fda084…	0 Ether	0.00472709
0x1e3e469d3be700376a…	Atomic Match_	13764968	58 secs ago	0xf88140b1f0fa5d21004…	OpenSea	0.079 Ether	0.01162145
0x753f4969841b56390a…	0xc04b8d59	13764968	58 secs ago	0xaa1076090ed9021d3a…	Uniswap V3: Router	0 Ether	0.01753823
0xd259c43906762569b6…	Approve	13764968	58 secs ago	0x50bce6bd28aba7e531…	Wrapped Ether	0 Ether	0.00262935
0x8b6fab43b2c7587cc37…	Deposit	13764968	58 secs ago	0x2fe55b3352c06c11ca7…	0xa760e26aa767470201…	0 Ether	0.00573802

Posljedice raspodijeljenog konzenzusa

- Svi čvorovi moraju izvršavati kod i provjeriti rezultat.
- Izvršavanje mora biti deterministično.
- Svaki poziv se mora izvršiti do kraja ili se ne izvršiti uopće.

Zadatak

Možete li:

- *dizajnirati pametni ugovor koji simulira klađenje na ishod bacanja novčića?*
- *dizajnirati pametni ugovor koji simulira klađenje na igru "par-nepar"?*

Gdje su poticaji za izvršavanje ugovora!

- Zašto bi rudar trošio resurse za izvršavanje ugovora kad može samo obrađivati *obične* transakcije?
- Što ako se poziv ugovora dugo (ili beskonačno) izvršava? Što ako troši nerazumnu količinu memorije?

Rješenje: gorivo

Inicijator transakcije plaća resurse potrebne za izvršavanje *gorivom*. U svakoj transakciji inicijator navodi:

- Gornji limit na količinu goriva predviđenog za izvršavanje transakcije.
- Cijenu naknade koju je voljan platiti po jedinici goriva.

Pametni ugovori – neka preostala pitanja

- Kako nastaje ugovor?
- Može li ugovor nestati?
- Može li ugovor kreirati transakciju?
- Ima li ugovor kriptografske ključeve?
- Kako točno izvršavanje troši gorivo?
- Što se točno događa ako se pozove beskonačna petlja?

Jednostavan jednodretveni virtualni stroj baziran na stogu.

Podaci

- Bytecode programa koji se izvršava (*read only*).
- Trajna memorija (dio globalnog stanja).
- Privremena memorija.
- Privremeni stog.

Instrukcije

- Aritmetičko-logičke, operacije (`ADD`, `MUL`, `SHA3`, ...).
- Operacije sa stogom (`POP`, `LOADM`, `DUP2`, ...).
- Kontrola toka programa (`STOP`, `JUMP`, `JUMPI`, ...).
- Sistemske operacije (`CREATE`, `CALL`, `RETURN`, ...).
- Dohvat informacija iz transakcije ili bloka (`CALLER`, `BALANCE`, `NUMBER`, ...)

Bug-ovi su skupi!

Pametni ugovor vjerojatno ne želite ručno pisati u bytecode-u.

Specijalizirani programski jezici

- Solidity: objektno-orijentirani jezik, sintaksom sličan Javi.
- LLL: funkcijski jezik, sintaksom sličan Lispu.
- Serpent: imperativni jezik, sintaksom sličan Python-u.
- Vyper: funkcijski jezik, sintaksom sličan Python-u.

Ugovor se sastoji od funkcija i podataka.

Storage

```
contract SimpleStorage {
    uint storedData;
    function set(uint x) public {
        storedData = x;
    }
    function get() public view returns (uint) {
        return storedData;
    }
  }
```

Izvor: `solidity.readthedocs.io`

Ugovor može slati i primati sredstva.

Faucet.sol

```
contract Faucet {
    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {
        // Limit withdrawal amount
        require(withdraw_amount <= 10000000000000000);
        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
    }
    // Accept any incoming amount
    function () public payable {}
}
```

Izvor: github.com/ethereumbook

Jesu li pozivi funkcija dio specifikacije virtualnog stroja?

The Contract Application Binary Interface (ABI)

Dogovoreni način interakcije s ugovorima na Ethereum platformi – prilikom pozivanja ugovora iz transakcija i iz drugog ugovora.

Specifikacija (otprilike):

- Prva četiri byte-a *data* polja u transakciji označavaju funkciju koja se poziva.
- Oznaka funkcije su prva četiri byte-a Keccak-256 sažetka njezinog prototipa.
- Ostatak *data* polja sadrži enkodirane parametre funkcije koja se zove.

Tipovi podataka

- Boolean (bool)
- Integer (int, uint, uint8, . . . , uint256)
- Fixed point (fixed, ufixed)
- Address (A 20-byte Ethereum address)
- Byte array (fixed or dynamic)
- Enum
- Arrays
- Struct
- Mapping (hash tablica)

Izražavanje konstantnih vrijednosti

- Vremenske jedinice (seconds, minites, hours, days)
- Ether novčane jedinice (wei, finney, szabo, ether)

Coin

```
contract Coin {
    address public minter;
    mapping (address => uint) public balances;

    constructor() public {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        require(amount < 1e60);
        balances[receiver] += amount;
    }

    function send(address receiver, uint amount) public {
        require(amount <= balances[msg.sender], "Insufficient balance.");
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
    }
}
```

Izvor: `solidity.readthedocs.io`

Zadatak

Istražite kojih su najpopularniji ugovori na Ethereum platformi.

Zadatak

Pronađite neki pametni ugovor na Etherscan-u pisan u Solidity-u te proučite što radi i kako radi.

Zadatak

Istražite koliko je koštao najskuplji sigurnosni propust u pametnom ugovoru.

Zadatak

Istražite koliki su računalni resursi potrebni za čisto računanje na Ethereum platformi u usporedbi s vašim laptopom.